UNIVERSIDAD REY JUAN CARLOS

TRABAJO FIN DE GRADO

Aplicación para la compartición segura de ficheros

Autor:
Sergio Merino Hernández

Tutor:
Dr. Gorka Guardiola Múzquiz

ESCUELA TÉCNICA SUPERIOR DE INGENIERÍA DE TELECOMUNICACIÓN
GRADO EN INGENIERÍA EN TELEMÁTICA

17 de octubre de 2017

Resumen

The Thesis Abstract is written here (and usually kept to just this page). The page is kept centered vertically so can expand into the blank space above the title too…

Agradecimientos

The acknowledgments and the people to thank go here, don't forget to include your project advisor...

Índice general

Índice de figuras

Índice de cuadros

Lista de Abreviaciones

LAH	**L**ist **A**bbreviations **H**ere
WSF	**W**hat (it) **S**tands **F**or

For/Dedicated to/To my…

Capítulo 1

Uso de la plantilla

1.1. Welcome and Thank You

Welcome to this LaTeX Thesis Template, a beautiful and easy to use template for writing a thesis using the LaTeX typesetting system.

If you are writing a thesis (or will be in the future) and its subject is technical or mathematical (though it doesn't have to be), then creating it in LaTeX is highly recommended as a way to make sure you can just get down to the essential writing without having to worry over formatting or wasting time arguing with your word processor.

LaTeX is easily able to professionally typeset documents that run to hundreds or thousands of pages long. With simple mark-up commands, it automatically sets out the table of contents, margins, page headers and footers and keeps the formatting consistent and beautiful. One of its main strengths is the way it can easily typeset mathematics, even *heavy* mathematics. Even if those equations are the most horribly twisted and most difficult mathematical problems that can only be solved on a super-computer, you can at least count on LaTeX to make them look stunning.

1.2. Learning LaTeX

LaTeX is not a WYSIWYG (What You See is What You Get) program, unlike word processors such as Microsoft Word or Apple's Pages. Instead, a document written for LaTeX is actually a simple, plain text file that contains *no formatting*. You tell LaTeX how you want the formatting in the finished document by writing in simple commands amongst the text, for example, if I want to use *italic text for emphasis*, I write the `\emph{text}` command and put the text I want in italics in between the curly braces. This means that LaTeX is a «mark-up» language, very much like HTML.

1.2.1. A (not so short) Introduction to LaTeX

If you are new to LaTeX, there is a very good eBook – freely available online as a PDF file – called, «The Not So Short Introduction to LaTeX». The book's title is typically shortened to just *lshort*. You can download the latest version (as it is occasionally updated) from here: `http://www.ctan.org/tex-archive/info/lshort/english/lshort.pdf`

It is also available in several other languages. Find yours from the list on this page: `http://www.ctan.org/tex-archive/info/lshort/`

It is recommended to take a little time out to learn how to use LaTeX by creating several, small 'test' documents, or having a close look at several templates on: `http://www.LaTeXTemplates.com`

Making the effort now means you're not stuck learning the system when what you *really* need to be doing is writing your thesis.

1.2.2. A Short Math Guide for LaTeX

If you are writing a technical or mathematical thesis, then you may want to read the document by the AMS (American Mathematical Society) called, «A Short Math Guide for LaTeX». It can be found online here: `http://www.ams.org/tex/amslatex.html` under the «Additional Documentation» section towards the bottom of the page.

1.2.3. Common LaTeX Math Symbols

There are a multitude of mathematical symbols available for LaTeX and it would take a great effort to learn the commands for them all. The most common ones you are likely to use are shown on this page: `http://www.sunilpatel.co.uk/latex-type/latex-math-symbols/`

You can use this page as a reference or crib sheet, the symbols are rendered as large, high quality images so you can quickly find the LaTeX command for the symbol you need.

1.2.4. LaTeX on a Mac

The LaTeX distribution is available for many systems including Windows, Linux and Mac OS X. The package for OS X is called MacTeX and it contains all the applications you need – bundled together and pre-customized – for a fully working LaTeX environment and work flow.

MacTeX includes a custom dedicated LaTeX editor called TeXShop for writing your '`.tex`' files and BibDesk: a program to manage your references and create your bibliography section just as easily as managing songs and creating playlists in iTunes.

1.3. Getting Started with this Template

If you are familiar with LaTeX, then you should explore the directory structure of the template and then proceed to place your own information into the *THESIS INFORMATION* block of the `main.tex` file. You can then modify the rest of this file to your unique specifications based on your degree/university. Section 1.5 on page 4 will help you do this. Make sure you also read section 1.7 about thesis conventions to get the most out of this template.

If you are new to LaTeX it is recommended that you carry on reading through the rest of the information in this document.

Before you begin using this template you should ensure that its style complies with the thesis style guidelines imposed by your institution. In most cases this template style and layout will be suitable. If it is not, it may only require a small change to bring the template in line with your institution's recommendations. These modifications will need to be done on the `MastersDoctoralThesis.cls` file.

1.3.1. About this Template

This LaTeX Thesis Template is originally based and created around a LaTeX style file created by Steve R. Gunn from the University of Southampton (UK), department of Electronics and Computer Science. You can find his original thesis style file at his site, here: `http://www.ecs.soton.ac.uk/~srg/softwaretools/document/templates/`

Steve's `ecsthesis.cls` was then taken by Sunil Patel who modified it by creating a skeleton framework and folder structure to place the thesis files in. The resulting template can be found on Sunil's site here: `http://www.sunilpatel.co.uk/thesis-template`

Sunil's template was made available through `http://www.LaTeXTemplates.com` where it was modified many times based on user requests and questions. Version 2.0 and onwards of this template represents a major modification to Sunil's template and is, in fact, hardly recognisable. The work to make version 2.0 possible was carried out by Vel and Johannes Böttcher.

1.4. What this Template Includes

1.4.1. Folders

This template comes as a single zip file that expands out to several files and folders. The folder names are mostly self-explanatory:

Appendices – this is the folder where you put the appendices. Each appendix should go into its own separate `.tex` file. An example and template are included in the directory.

Chapters – this is the folder where you put the thesis chapters. A thesis usually has about six chapters, though there is no hard rule on this. Each chapter should go in its own separate `.tex` file and they can be split as:

- Chapter 1: Introduction to the thesis topic
- Chapter 2: Background information and theory
- Chapter 3: (Laboratory) experimental setup
- Chapter 4: Details of experiment 1
- Chapter 5: Details of experiment 2
- Chapter 6: Discussion of the experimental results
- Chapter 7: Conclusion and future directions

This chapter layout is specialised for the experimental sciences, your discipline may be different.

Figures – this folder contains all figures for the thesis. These are the final images that will go into the thesis document.

1.4.2. Files

Included are also several files, most of them are plain text and you can see their contents in a text editor. After initial compilation, you will see that more auxiliary

files are created by LaTeX or BibTeX and which you don't need to delete or worry about:

example.bib – this is an important file that contains all the bibliographic information and references that you will be citing in the thesis for use with BibTeX. You can write it manually, but there are reference manager programs available that will create and manage it for you. Bibliographies in LaTeX are a large subject and you may need to read about BibTeX before starting with this. Many modern reference managers will allow you to export your references in BibTeX format which greatly eases the amount of work you have to do.

MastersDoctoralThesis.cls – this is an important file. It is the class file that tells LaTeX how to format the thesis.

main.pdf – this is your beautifully typeset thesis (in the PDF file format) created by LaTeX. It is supplied in the PDF with the template and after you compile the template you should get an identical version.

main.tex – this is an important file. This is the file that you tell LaTeX to compile to produce your thesis as a PDF file. It contains the framework and constructs that tell LaTeX how to layout the thesis. It is heavily commented so you can read exactly what each line of code does and why it is there. After you put your own information into the *THESIS INFORMATION* block – you have now started your thesis!

Files that are *not* included, but are created by LaTeX as auxiliary files include:

main.aux – this is an auxiliary file generated by LaTeX, if it is deleted LaTeX simply regenerates it when you run the main `.tex` file.

main.bbl – this is an auxiliary file generated by BibTeX, if it is deleted, BibTeX simply regenerates it when you run the `main.aux` file. Whereas the `.bib` file contains all the references you have, this `.bbl` file contains the references you have actually cited in the thesis and is used to build the bibliography section of the thesis.

main.blg – this is an auxiliary file generated by BibTeX, if it is deleted BibTeX simply regenerates it when you run the main `.aux` file.

main.lof – this is an auxiliary file generated by LaTeX, if it is deleted LaTeX simply regenerates it when you run the main `.tex` file. It tells LaTeX how to build the *List of Figures* section.

main.log – this is an auxiliary file generated by LaTeX, if it is deleted LaTeX simply regenerates it when you run the main `.tex` file. It contains messages from LaTeX, if you receive errors and warnings from LaTeX, they will be in this `.log` file.

main.lot – this is an auxiliary file generated by LaTeX, if it is deleted LaTeX simply regenerates it when you run the main `.tex` file. It tells LaTeX how to build the *List of Tables* section.

main.out – this is an auxiliary file generated by LaTeX, if it is deleted LaTeX simply regenerates it when you run the main `.tex` file.

So from this long list, only the files with the `.bib`, `.cls` and `.tex` extensions are the most important ones. The other auxiliary files can be ignored or deleted as LaTeX and BibTeX will regenerate them.

1.5. Filling in Your Information in the `main.tex` File

You will need to personalise the thesis template and make it your own by filling in your own information. This is done by editing the `main.tex` file in a text editor or your favourite LaTeX environment.

Open the file and scroll down to the third large block titled *THESIS INFORMATION* where you can see the entries for *University Name*, *Department Name*, etc ...

Fill out the information about yourself, your group and institution. You can also insert web links, if you do, make sure you use the full URL, including the `http://` for this. If you don't want these to be linked, simply remove the `\href{url}{name}` and only leave the name.

When you have done this, save the file and recompile `main.tex`. All the information you filled in should now be in the PDF, complete with web links. You can now begin your thesis proper!

1.6. The `main.tex` File Explained

The `main.tex` file contains the structure of the thesis. There are plenty of written comments that explain what pages, sections and formatting the LaTeX code is creating. Each major document element is divided into commented blocks with titles in all capitals to make it obvious what the following bit of code is doing. Initially there seems to be a lot of LaTeX code, but this is all formatting, and it has all been taken care of so you don't have to do it.

Begin by checking that your information on the title page is correct. For the thesis declaration, your institution may insist on something different than the text given. If this is the case, just replace what you see with what is required in the *DECLARATION PAGE* block.

Then comes a page which contains a funny quote. You can put your own, or quote your favourite scientist, author, person, and so on. Make sure to put the name of the person who you took the quote from.

Following this is the abstract page which summarises your work in a condensed way and can almost be used as a standalone document to describe what you have done. The text you write will cause the heading to move up so don't worry about running out of space.

Next come the acknowledgements. On this page, write about all the people who you wish to thank (not forgetting parents, partners and your advisor/supervisor).

The contents pages, list of figures and tables are all taken care of for you and do not need to be manually created or edited. The next set of pages are more likely to be optional and can be deleted since they are for a more technical thesis: insert a list of abbreviations you have used in the thesis, then a list of the physical constants and numbers you refer to and finally, a list of mathematical symbols used in any formulae. Making the effort to fill these tables means the reader has a one-stop place to refer to instead of searching the internet and references to try and find out what you meant by certain abbreviations or symbols.

The list of symbols is split into the Roman and Greek alphabets. Whereas the abbreviations and symbols ought to be listed in alphabetical order (and this is *not* done automatically for you) the list of physical constants should be grouped into similar themes.

The next page contains a one line dedication. Who will you dedicate your thesis to?

Finally, there is the block where the chapters are included. Uncomment the lines (delete the % character) as you write the chapters. Each chapter should be written in its own file and put into the *Chapters* folder and named `Chapter1`, `Chapter2`, etc... Similarly for the appendices, uncomment the lines as you need them. Each appendix should go into its own file and placed in the *Appendices* folder.

After the preamble, chapters and appendices finally comes the bibliography. The bibliography style (called *authoryear*) is used for the bibliography and is a fully featured style that will even include links to where the referenced paper can be found online. Do not underestimate how grateful your reader will be to find that a reference to a paper is just a click away. Of course, this relies on you putting the URL information into the BibTeX file in the first place.

1.7. Thesis Features and Conventions

To get the best out of this template, there are a few conventions that you may want to follow.

One of the most important (and most difficult) things to keep track of in such a long document as a thesis is consistency. Using certain conventions and ways of doing things (such as using a Todo list) makes the job easier. Of course, all of these are optional and you can adopt your own method.

1.7.1. Printing Format

This thesis template is designed for double sided printing (i.e. content on the front and back of pages) as most theses are printed and bound this way. Switching to one sided printing is as simple as uncommenting the *oneside* option of the `documentclass` command at the top of the `main.tex` file. You may then wish to adjust the margins to suit specifications from your institution.

The headers for the pages contain the page number on the outer side (so it is easy to flick through to the page you want) and the chapter name on the inner side.

The text is set to 11 point by default with single line spacing, again, you can tune the text size and spacing should you want or need to using the options at the very start of `main.tex`. The spacing can be changed similarly by replacing the *singlespacing* with *onehalfspacing* or *doublespacing*.

1.7.2. Using US Letter Paper

The paper size used in the template is A4, which is the standard size in Europe. If you are using this thesis template elsewhere and particularly in the United States, then you may have to change the A4 paper size to the US Letter size. This can be done in the margins settings section in `main.tex`.

Due to the differences in the paper size, the resulting margins may be different to what you like or require (as it is common for institutions to dictate certain margin sizes). If this is the case, then the margin sizes can be tweaked by modifying the values in the same block as where you set the paper size. Now your document should be set up for US Letter paper size with suitable margins.

1.7.3. References

The `biblatex` package is used to format the bibliography and inserts references such as this one (Hawthorn, Weber y Scholten, 2001). The options used in the `main.tex` file mean that the in-text citations of references are formatted with the author(s) listed with the date of the publication. Multiple references are separated by semicolons (e.g. (Wieman y Hollberg, 1991; Hawthorn, Weber y Scholten, 2001)) and references with more than three authors only show the first author with *et al.* indicating there are more authors (e.g. (Arnold y col., 1998)). This is done automatically

for you. To see how you use references, have a look at the `Chapter1.tex` source file. Many reference managers allow you to simply drag the reference into the document as you type.

Scientific references should come *before* the punctuation mark if there is one (such as a comma or period). The same goes for footnotes[1]. You can change this but the most important thing is to keep the convention consistent throughout the thesis. Footnotes themselves should be full, descriptive sentences (beginning with a capital letter and ending with a full stop). The APA6 states: «Footnote numbers should be superscripted, [...], following any punctuation mark except a dash.» The Chicago manual of style states: «A note number should be placed at the end of a sentence or clause. The number follows any punctuation mark except the dash, which it precedes. It follows a closing parenthesis.»

The bibliography is typeset with references listed in alphabetical order by the first author's last name. This is similar to the APA referencing style. To see how LaTeX typesets the bibliography, have a look at the very end of this document (or just click on the reference number links in in-text citations).

A Note on bibtex

The bibtex backend used in the template by default does not correctly handle unicode character encoding (i.e. ïnternationalçharacters). You may see a warning about this in the compilation log and, if your references contain unicode characters, they may not show up correctly or at all. The solution to this is to use the biber backend instead of the outdated bibtex backend. This is done by finding this in `main.tex`: *`backend=bibtex`* and changing it to *`backend=biber`*. You will then need to delete all auxiliary BibTeX files and navigate to the template directory in your terminal (command prompt). Once there, simply type `biber main` and biber will compile your bibliography. You can then compile `main.tex` as normal and your bibliography will be updated. An alternative is to set up your LaTeX editor to compile with biber instead of bibtex, see here for how to do this for various editors.

1.7.4. Tables

Tables are an important way of displaying your results, below is an example table which was generated with this code:

```
\begin{table}
\caption{The effects of treatments X and Y on the four groups studied.}
\label{tab:treatments}
\centering
\begin{tabular}{l l l}
\toprule
\tabhead{Groups} & \tabhead{Treatment X} & \tabhead{Treatment Y} \\
\midrule
1 & 0.2 & 0.8\\
2 & 0.17 & 0.7\\
3 & 0.24 & 0.75\\
4 & 0.68 & 0.3\\
\bottomrule\\
\end{tabular}
\end{table}
```

[1] Such as this footnote, here down at the bottom of the page.

CUADRO 1.1: The effects of treatments X and Y on the four groups studied.

Groups	Treatment X	Treatment Y
1	0.2	0.8
2	0.17	0.7
3	0.24	0.75
4	0.68	0.3

You can reference tables with `\ref{<label>}` where the label is defined within the table environment. See `Chapter1.tex` for an example of the label and citation (e.g. Table 1.1).

1.7.5. Figures

There will hopefully be many figures in your thesis (that should be placed in the *Figures* folder). The way to insert figures into your thesis is to use a code template like this:

```
\begin{figure}
\centering
\includegraphics{Figures/Electron}
\decoRule
\caption[An Electron]{An electron (artist's impression).}
\label{fig:Electron}
\end{figure}
```

Also look in the source file. Putting this code into the source file produces the picture of the electron that you can see in the figure below.

Sometimes figures don't always appear where you write them in the source. The placement depends on how much space there is on the page for the figure. Sometimes there is not enough room to fit a figure directly where it should go (in relation to the text) and so LaTeX puts it at the top of the next page. Positioning figures is the job of LaTeX and so you should only worry about making them look good!

Figures usually should have captions just in case you need to refer to them (such as in Figure 1.1). The `\caption` command contains two parts, the first part, inside the square brackets is the title that will appear in the *List of Figures*, and so should be short. The second part in the curly brackets should contain the longer and more descriptive caption text.

The `\decoRule` command is optional and simply puts an aesthetic horizontal line below the image. If you do this for one image, do it for all of them.

LaTeX is capable of using images in pdf, jpg and png format.

1.7.6. Typesetting mathematics

If your thesis is going to contain heavy mathematical content, be sure that LaTeX will make it look beautiful, even though it won't be able to solve the equations for you.

The «Not So Short Introduction to LaTeX» (available on CTAN) should tell you everything you need to know for most cases of typesetting mathematics. If you need

FIGURA 1.1: An electron (artist's impression).

more information, a much more thorough mathematical guide is available from the AMS called, «A Short Math Guide to LaTeX» and can be downloaded from: `ftp://ftp.ams.org/pub/tex/doc/amsmath/short-math-guide.pdf`

There are many different LaTeX symbols to remember, luckily you can find the most common symbols in The Comprehensive LaTeX~Symbol List.

You can write an equation, which is automatically given an equation number by LaTeX like this:

```
\begin{equation}
E = mc^{2}
\label{eqn:Einstein}
\end{equation}
```

This will produce Einstein's famous energy-matter equivalence equation:

$$E = mc^2 \tag{1.1}$$

All equations you write (which are not in the middle of paragraph text) are automatically given equation numbers by LaTeX. If you don't want a particular equation numbered, use the unnumbered form:

```
\[ a^{2}=4 \]
```

1.8. Sectioning and Subsectioning

You should break your thesis up into nice, bite-sized sections and subsections. LaTeX automatically builds a table of Contents by looking at all the `\chapter{}`, `\section{}` and `\subsection{}` commands you write in the source.

The Table of Contents should only list the sections to three (3) levels. A `chapter{}` is level zero (0). A `\section{}` is level one (1) and so a `\subsection{}` is level two (2). In your thesis it is likely that you will even use a `subsubsection{}`, which is level three (3). The depth to which the Table of Contents is formatted is set within `MastersDoctoralThesis.cls`. If you need this changed, you can do it in `main.tex`.

1.9. In Closing

You have reached the end of this mini-guide. You can now rename or overwrite this pdf file and begin writing your own `Chapter1.tex` and the rest of your thesis. The easy work of setting up the structure and framework has been taken care of for you. It's now your job to fill it out!

Good luck and have lots of fun!

Guide written by —
Sunil Patel: www.sunilpatel.co.uk
Vel: LaTeXTemplates.com

Capítulo 2

Introducción

2.1. Motivación

Las comunicaciones seguras nacen del deseo de protegernos: de proteger con quién nos comunicamos y el qué comunicamos.

De este deseo surgen multitud de protocolos de seguridad que hoy en día usamos sin darnos cuenta. Desde una simple consulta web hasta la felicitación de Año Nuevo, nuestras comunicaciones pasan por diversas operaciones para preservar su seguridad.

Esta seguridad viene generalmente proporcionada por la confianza que depositamos en ciertas organizaciones, las cuales crean una red de confianza sobre la que se sustenta todo este sistema. Pero, ¿qué sucede si no podemos confiar en estas entidades? ¿Y si queremos ser nosotros los responsables de proporcionar la seguridad?

Con esta idea comienza la búsqueda de una herramienta que permita a los usuarios ser los artífices de su propia red de confianza, el pilar central en seguridad.

2.2. Estructura de la memoria

Capítulo 3

Objetivos

3.1. Objetivo general

3.2. Objetivos específicos

3.3. Modelo de atacante

Capítulo 4

Estado del Arte

4.1. Java

Java es un lenguaje de programación de propósito general, concurrente, orientado a objetos y diseñado específicamente para tener tan pocas dependencias de implementación como fuera posible.

Su intención es permitir que los desarrolladores de aplicaciones escriban el programa una vez y lo puedan ejecutar en cualquier dispositivo (conocido en inglés como *WORA*, o "*write once, run anywhere*"), lo que quiere decir que el código que es ejecutado en una plataforma no necesita ser recompilado para correr en otra. *(Wikipedia, 2017c)*

FIGURA 4.1: Logo de Java

4.2. Android

Android es un sistema operativo basado en el núcleo Linux, diseñado principalmente para dispositivos móviles con pantalla táctil, como *smartphones* y *tablets*.

Aunque la mayoría de las aplicaciones están escritas en Java, no hay una máquina virtual Java en la plataforma. El bytecode Java no es ejecutado, sino que primero

se compila en un ejecutable Dalvik y se ejecuta en la Máquina Virtual Dalvik[1]. A partir de la versión 5.0, se utiliza el Android Runtime (ART). *(Wikipedia, 2017a)*

FIGURA 4.2: Logo de Android

4.3. Bouncy Castle

Bouncy Castle (BC), también llamado Bouncy Castle Crypto, es una colección de APIs utilizados en criptografía. Tiene versiones para los lenguajes Java y C#.

La arquitectura de BC consta de dos componentes principales que soportan las prestaciones básicas de criptografía. Estos son una API *ligera* y un proveedor para Java Cryptography Extension (JCE)[2]. Otros componentes basados en el proveedor para JCE admiten funciones adicionales, como soporte para PGP, S/MIME, etc. *(Wikipedia, 2017b)*

FIGURA 4.3: The Legion of Bouncy Castle, creadores de Bouncy Castle

4.4. Padding

Padding es el nombre que recibe la técnica que permite en criptografía por bloques expandir el último bloque del mensaje hasta lograr el tamaño requerido.

Existen múltiples técnicas de padding. Bruce Schenier, en su libro *Cryptography Engineering*, menciona dos:

[1]Dalvik es una máquina virtual especializada, diseñada específicamente para Android y optimizada para dipositivos móviles que funcionan con batería y que tienen memoria y procesador limitados.

[2]JCE implementa encriptación, generación y protocolos de establecimiento de claves y algoritmos MAC.

- Agregar al final del mensaje un byte con el valor 128 y luego agregar tantos 0's como haga falta para alcanzar el largo del *bloque de largo fijo*.
- Determinar el número de bytes que se requieren de padding. Supongamos que este número es **n**. Completar el mensaje con **n** bytes de valor **n**.

Cualquier técnica es válida mientras permita completar el mensaje hasta el largo requerido y el receptor pueda obtener con exactitud el mensaje original. *(Balao, 2011)*

4.5. Criptografía de clave pública

La **criptografía de clave pública**, también llamada criptografía asimétrica, es el método criptográfico que usa un par de claves para la firma y el cifrado de mensajes. Una clave es *pública* y se puede entregar a cualquier persona, la otra clave es *privada* y el propietario debe guardarla de modo que nadie tenga acceso a ella.

Si el remitente usa la clave pública del destinatario para cifrar el mensaje, una vez cifrado, sólo la clave privada del destinatario podrá descifrar este mensaje, ya que es el único que la conoce. Por tanto se logra la *confidencialidad* del envío del mensaje, nadie salvo el destinatario puede descifrarlo.

Si el propietario del par de claves usa su clave privada para cifrar el mensaje, cualquiera puede descifrarlo utilizando su clave pública. En este caso se consigue por tanto la *identificación* y *autentificación* del remitente, ya que se sabe que sólo pudo haber sido él quien empleó su clave privada (salvo que alguien se la hubiese podido robar). Esta idea es el fundamento de la firma electrónica[3]. *(Wikipedia, 2017d)*

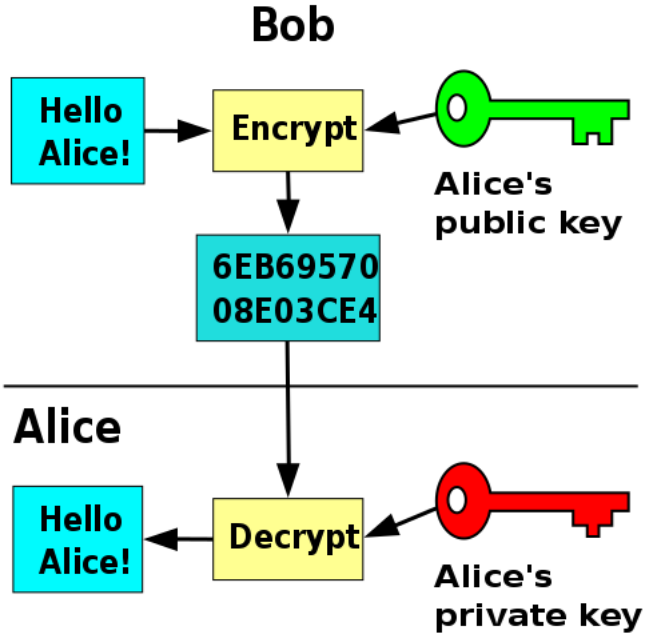

FIGURA 4.4: Esquema general del cifrado de clave pública

[3]Existen multitud de algoritmos de firma, para este proyecto se ha optado por usar RSASSA-PSS.

4.6. RSA

RSA (**Rivest–Shamir–Adleman**)[4] es uno de los primeros sistemas de criptografía de clave pública y es ampliamente utilizado para la transmisión segura de datos. En RSA, la asimetría que existe entre las claves pública y privada se basa en la dificultad práctica de la factorización del producto de dos grandes números primos (*factoring problem*). *(Wikipedia, 2017e)*

4.6.1. Clave pública RSA

Una **clave pública RSA** consta de dos componentes:

- **n** – el módulo RSA, un entero positivo.
- **e** – el exponente público RSA, un entero positivo.

En una **clave pública RSA** válida, **n** es un producto de **u**[5] números primos impares distintos

$$r_i, i = 1, 2, ..., u$$

, donde **u** >= 2, y **e** es un entero entre 3 y **n** - 1, satisfaciendo

$$MCD(e, \lambda(n)) = 1$$

, donde

$$\lambda(n)^6 = mcm(r_1 - 1, ..., r_u - 1)$$

Por convención, los dos primeros números primos se denotan como p y q, respectivamente. *(Jonsson y Kaliski, 2003)*

4.6.2. Clave privada RSA

4.7. RSASSA-PSS

4.8. Criptografía de clave simétrica

4.9. Cifrado de bloques

4.10. CBC

4.11. AES

4.12. HTTP

[4] El acrónimo RSA está compuesto por las letras iniciales de los apellidos de Ron Rivest, Adi Shamir y Leonard Adleman, quienes primero describieron públicamente el algoritmo en 1978.

[5] La ventaja de usar más de dos factores primos es que tendríamos un menor coste computacional para el desencriptador y las primitivas de firma.

[6] Función de Carmichael.

Capítulo 5

Diseño e implementación

5.1. Arquitectura de seguridad

5.2. Arquitectura del software

Capítulo 6

Resultados

6.1. Ejemplos de utilidad

6.2. Problemas encontrados

Capítulo 7

Conclusiones finales

7.1. Objetivos alcanzados

7.2. Líneas futuras

Apéndice A

Frequently Asked Questions

A.1. How do I change the colors of links?

The color of links can be changed to your liking using:
`\hypersetup{urlcolor=red}`, or
`\hypersetup{citecolor=green}`, or
`\hypersetup{allcolor=blue}`.
If you want to completely hide the links, you can use:
`\hypersetup{allcolors=.}`, or even better:
`\hypersetup{hidelinks}`.
If you want to have obvious links in the PDF but not the printed text, use:
`\hypersetup{colorlinks=false}`.

Bibliografía

Arnold, A. S. y col. (1998). «A Simple Extended-Cavity Diode Laser». En: *Review of Scientific Instruments* 69.3, págs. 1236-1239. URL: http://link.aip.org/link/?RSI/69/1236/1.

Balao, Martín (2011). *Criptografía: Padding + ECB + CBC*. URL: http://martin.com.uy/sec/criptografia-padding-ecb-cbc/.

Hawthorn, C. J., K. P. Weber y R. E. Scholten (2001). «Littrow Configuration Tunable External Cavity Diode Laser with Fixed Direction Output Beam». En: *Review of Scientific Instruments* 72.12, págs. 4477-4479. URL: http://link.aip.org/link/?RSI/72/4477/1.

Jonsson, J. y B. Kaliski (2003). *Public-Key Cryptography Standards (PKCS) 1: RSA Cryptography Specifications Version 2.1*. Inf. téc. RFC 3447. IETF, pág. 6. URL: https://tools.ietf.org/html/rfc3447#section-3.

Wieman, Carl E. y Leo Hollberg (1991). «Using Diode Lasers for Atomic Physics». En: *Review of Scientific Instruments* 62.1, págs. 1-20. URL: http://link.aip.org/link/?RSI/62/1/1.

Wikipedia (2017a). *Android*. URL: https://es.wikipedia.org/wiki/Android.

— (2017b). *Bouncy Castle (cryptography)*. URL: https://en.wikipedia.org/wiki/Bouncy_Castle_(cryptography).

— (2017c). *Java (programming language)*. URL: https://en.wikipedia.org/wiki/Java_(programming_language).

— (2017d). *Public-key cryptography*. URL: https://en.wikipedia.org/wiki/Public-key_cryptography.

— (2017e). *RSA (cryptosystem)*. URL: https://en.wikipedia.org/wiki/RSA_(cryptosystem).